WILLIAM L. ANTHONY (State Bar No. 106908)
ERIC L. WESENBERG (State Bar No. 139696)
KENNETH J. HALPERN (State Bar No. 187663)
ORRICK, HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

STEVEN ALEXANDER (admitted *Pro Hac Vice*)
KRISTIN L. CLEVELAND (admitted *Pro Hac Vice*)
JAMES E. GERINGER (admitted *Pro Hac Vice*)
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446

Attorneys for Defendant and Counterclaimant,
MICROSOFT CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation,

Plaintiff,

v.

MICROSOFT CORPORATION, a Washington corporation,

Defendant.

MICROSOFT CORPORATION, a Washington corporation,

Counterclaimant,

v.

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation,

Counter Claim-Defendant.

Case No. C 01-1640 SBA (MEJ)

Consolidated with C 02-0647 SBA (MEJ)

REPLY TO INTERTRUST'S OPPOSITION TO MICROSOFT'S BRIEF IN SUPPORT OF MOTION FOR SUMMARY JUDGMENT THAT CERTAIN "MINI-*MARKMAN*" CLAIMS ARE INVALID FOR INDEFINITENESS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

FEDERAL STATUTES

I. INTRODUCTION AND SUMMARY OF ARGUMENT

InterTrust's opposition brief throws up a storm of noise, diversion and straw arguments that should not distract this Court's attention from the very simple question on which the defense of indefiniteness will be determined: Whether the claim has sufficiently definite scope that a person of ordinary skill in the art can understand what it means in light of the specification and thereby determine what is outside its scope. *Union Pac. Resources Co. v. Chesapeake Energy Co.*, 236 F. 3d 684, 692 (Fed. Cir. 2001). For each of the eleven claims challenged on this motion, the answer must be, "No."

What emerges from InterTrust's opposition brief are two important points upon which the parties agree: First, "secure" is a relative term that has only a vague, general meaning in the art, which can mean different things in different contexts. Second, to determine what is "secure" in any particular context one of skill in the art needs specific criteria. The essential problem with InterTrust's patents is that they fail to provide the needed context and they fail to adopt any particular criteria, leaving both critical steps for others to guess at. They further fail to define "secure" expressly, and they fail to define it implicitly by identifying any particular technology used to achieve security. When one turns to the Big Book for resolution of the resulting ambiguity, it is like coming to a trailhead with 50 signs labeled "secure," but each pointing in a different, inconsistent, and often times contradictory direction.

The term "secure" is unusual in that it is a label characterizing a multidimensional condition of something – a result achieved amid constantly changing circumstances. It is an inherently subjective concept that can be evaluated in many different ways (with correspondingly different outcomes). Labels set forth in patent claims, however, must be subject to an objective evaluation. Otherwise, it is impossible for the public to evaluate the scope of the claim.

The ***claims*** fail to recite either context or criteria. The traditional places to which one turns to correct this shortcoming are equally unavailing. The evidence from the parties' experts, corroborated by third party accounts, confirms that definite context and criteria is critical information for anyone having skill in this art, and it is information that merely having skill in the art does ***not provide***. To the contrary, persons of skill in the art are aware of a multitude of

possible ways of distinguishing between something that is "secure" and something that is "not secure." Finally, ***the specification*** is equivocal on everything except what "VDE" can do, and the file history offers no resolution. Indeed, the specification compounds the problem because it mentions but fails to adopt any of the many possible security contexts and criteria. After reading the nearly one thousand pages of Big Book text, the person of ordinary skill in the art would have no idea what, for example, a claim's "secure container," "secure memory," or "secure process" must protect, or against what threats, or to what degree, or by what criteria such evaluations should be conducted. The evidence from the parties' experts, corroborated by third party accounts, confirms that specific context and criteria are critical information for anyone having skill in this art, and it is information that merely having skill in the art does ***not provide***. It is for these reasons that the mini-*Markman* claims are indefinite and should be declared invalid.

II. "SECURE" AS USED IN THESE MINI-MARKMAN CLAIMS RENDERS THEM INDEFINITE

A. A Person of Skill Reading the Claims Cannot Tell What "Secure" Means in Light of the Relevant Art

One of skill in the art reading the claims finds references to "secure memory," "secure database," "secure container," "securely assembling," and "level of security," but no explanation of what is meant by "secure" other than the promises made for the "present invention," "VDE." Looking to the art as a whole for guidance offers no comfort. The term, *as InterTrust admits*, has only a very general meaning – that some designs, techniques or mechanisms are used to protect certain properties against some kind of attack or adversarial conditions. InterTrust Opp., at 4 (quoting Prof. Mitchell's definition as the one on which both parties' experts "agree"). This definition manifestly lacks a clear boundary. Which designs, techniques, mechanisms, properties, attacks, and or conditions are intended? The claims point to no criteria in the art that would answer that question.

Both parties' experts agree that criteria are needed to reach a precise understanding of "secure." The testimony of InterTrust's own expert, cited in Microsoft's opening brief, fully supports the proposition that the term needs further specification of parameters and criteria in

order to be sufficiently definite.[1] Microsoft Brief, at 4. InterTrust's expert now adds that to apply the general meaning of "secure" "to a particular product or system, it is necessary to understand the context of that product or system." Reiter Decl., at ¶ 3. Dr. Reiter also admits that there are "several recognized methodologies for determining if computer products are 'secure'" and that "[c]omputer security professionals routinely use such methods to determine if products or methods are 'secure.'" Opp., at 3; Reiter Decl., at ¶ 3. InterTrust even approvingly characterizes Dr. Mitchell's testimony as meaning that one must know the protected properties and potential attacks to determine if a particular system is "secure," and that recognized methodologies are used to perform this investigation. *Id.* at 5. The Mitchell declaration, scholarly articles, and third-party witnesses have provided evidence to the same effect. *Id.*; Mitchell Decl., at 4-11.[2]

It should be noted here that InterTrust's allegation that Prof. Mitchell did not try to understand the terms in the context of the claims is based on a misrepresentation of his testimony. As Prof. Mitchell clearly explained, for each term and phrase in question, he "tired to look at its meaning in three different ways" – whether the term by itself has a commonly understood specific meaning, whether the term is clear "in the context of the claim," and whether the patent specification provides "any further information." (Mitchell Depo. at 294). In its brief, however, InterTrust cut off the quotation of Prof. Mitchell's testimony right before he gave an answer that contradicted the proposition for which InterTrust quoted him:

> A. I – I tried to explain a little bit earlier that my task to this point in this case has been to, first of all, understand the patent's specs and so on, and, second, in particular to this declaration, think about these particular phrases, what they mean in general, what they appear to mean in the claims, and ponder the question of whether the specification gives us additional useful information so that I could pin down the meaning of these terms in a useful and meaningful way.

---

[1] InterTrust erects Prof. Mitchell's effort to summarize the different axes of security into a classic straw man. Calling it a "test" – a term nowhere used by Microsoft – InterTrust reasons that, because this "test" is not recognized as such in the art, it sheds no light on the definiteness of InterTrust's patent claims.

[2] For this reason, InterTrust's lengthy argument that "secure" has a meaning in the art is beside the point. InterTrust Opp., at 2-3. As Microsoft stated in its opening brief, "while communicating a general or conceptual meaning, the term 'secure' lacks any precise, uniform definition to inform a person of skill in the art what it means *unless a number of questions are answered.*" Microsoft's Brief in Support of Motion, at 3 (emphasis added).

> In that process, I have read the claims and have some understanding of what they appear to promise and what they seem to mean in general. But as far as doing further detailed analysis of what is exactly required by each claim, I haven't really studied that in -- in a proper way yet.

Wesenberg Reply Decl., Exh. A (Mitchell Depo., Vol. 2, at 299:1-17).

Because the challenged claims use "secure" without providing specific parameters or criteria or referencing any in the art, one cannot determine their scope by reading them. A person of ordinary skill is left unable to define "secure" in light of the art and thus unable to understand the claims precisely enough to know what is in their scope.

B. The Specification Does Not Select Any Criteria for Evaluating "Secure", Though It Refers to Some

Faced with a vague and general "ordinary" meaning, we look to the patent specifications to see if they point to any of the criteria recognized in the art. InterTrust and Microsoft have identified some of the well-known "off-the-shelf" standards for determining "security," including the Common Criteria for Information Technology Security Evaluation, the Trusted Computer System Evaluation Criteria ("TCSEC"), and Federal Information Processing Standard 140-1 ("FIPS 140-1"). InterTrust Brief, p. 3; Reiter Decl., pp. 3-7. The fatal problem with InterTrust's specifications is that while they mention some of these standards, they adopt none of them. Nowhere is there a clear indication that a particular standard or identified criteria is the one to follow. The specification treats them as optional and applicable, if at all, only to a small part of the universe of the patent.

The TCSEC, for instance is mentioned in one column of the '193 patent, in a discussion of the possible use of VDE to support document management for a large organization. In a list of examples of how "VDE-enforced control capabilities" can be used to manage documents, the specification states that one particular type of document transmission channel and one type of storage device "could be" set up with restrictions that would satisfy the Device Labels requirement of the TCSEC. '193, col. 279:45-60. But these are just two examples (out of nine) of uses to which VDE can supposedly be put in one type of customer context, out of a great many others promised in the patent. Nowhere does the patent state or even suggest that TCSEC or any

part of it is meant to provide criteria to define "secure" throughout the patent, and interTrust does not make that argument now.

Likewise, the '721 specification mentions the FIPS-186 "Digital Signature Standard," but only as one possible methodology for evaluating the "security" of a digital signature. Again, InterTrust does not even argue that this is the standard a person of skill should use to evaluate whether something is "secure," but merely that one could do so.

C. **The Specification Does Not Define "Secure" for Purposes of the Patent**

Lacking a known criteria or a specified new criteria, an otherwise indefinite claim can be saved if the specification defines the proper measure of the problem term. Unfortunately, the 900+ pages of the patent specification point in so many different directions that it is impossible to know which apparent definition of "secure" to use. The patent does contain a great deal of verbiage about security methods and degrees. But its discussion of these issues is tantamount to a recitation of almost everything security could possibly mean or include, including unbounded references to whatever is not expressly recited in the patent.

1. **The Specification Does Not Define "Secure" Explicitly**

The patent never explicitly defines what "secure" means, either lexically or by outlining its own security policy or set of security criteria, a fact which InterTrust has not disputed.

2. **The Specification Does Not Define "Secure" by Functional Description**

The specification also fails to give "secure" a precise and unambiguous meaning by describing it functionally. That is, no clear and precise meaning of "secure" can be derived from the technological features disclosed in the specification. Although the specification contains a voluminous recitation of detail, that detail itself describes so many purportedly different levels of "security" that it is impossible to tell which technological features suffice to make a system "secure" in any particular instance. (As discussed below, it is inconsistent for InterTrust to argue that the specification provides the detail needed to make "secure" definite enough to determine what infringes, when it has excluded any such detail from its proposed Markman definition of the same term.)

The discussion of encryption mechanisms cited by InterTrust as supposed evidence of secure's definiteness exemplifies this. InterTrust argues that the '193 patent "contains a passage contrasting 'highly secure' encryption algorithms with 'extremely secure' algorithms, and explicitly identifies each type of algorithm, including explaining circumstances under which each should be used." InterTrust's opposition brief blithely reassures the reader that "both 'highly secure' and 'extremely secure' algorithms are 'secure.'" But these phrases clearly denote different degrees of security. To which level do the claims refer when they employ "secure"? InterTrust's answer that the specification tells one which "secure" mechanisms to use under which circumstances is untrue. The "highly secure" algorithm in this example is described simply as a "'bulk encryption/decryption technique.'" '193, col. 67:18-19. Elsewhere, the patent states that VDE "does not require any specific algorithm ... for bulk encryption/decryption." '193, Col. 201:27-29. More importantly, for both the "highly secure" and "extremely secure" cases, the measures mentioned are described as "preferable." *Id.*, col. 67:18, 21. This implies that there are circumstances under which the "preferable" option would not be employed, raising the question of what those circumstances are, who would make the decision, and how.

The next example cited by InterTrust begins to answer that question: in fact, "secure" is not evaluated by anything intrinsic to the patent, but by a subjective and unpredictable decisionmaking process. A discussion of encryption techniques that InterTrust offers as proof of the specificity with which the patent allegedly endows "secure," InterTrust Opp., at 6; '193, col. 201:63-202:12, is immediately preceded by this explanation:

> VDE 100 provided by the preferred embodiment accommodates and can use many different key lengths. The length of keys used by VDE 100 in the preferred embodiment is determined by the algorithm(s) used for encryption/decryption, ***the level of security desired***, and throughput requirements. Longer keys generally require additional processing power to ensure fast encryption/ decryption response times. Therefore, there is a tradeoff between (a) security, and (b) processing time and/or resources. Since a hardware-based PPE encrypt/decrypt engine 522 may provide faster processing than software-based encryption/decryption, the hardware-based approach may, in general, allow use of longer keys.

'193, Col. 201:50-62. There is no constraint placed on the "level of security desired" – it is up to the user or system designer (or someone – the patent does not say whom) to balance security

against their subjectively perceived costs in deciding what key lengths to use. The entire discussion of key lengths that follows is therefore dependent on a preference external to the patent. It is not enough to give technical details about key lengths, because whatever key length a person of skill in the art might choose or encounter fails to answer the question whether the product or activity in question is or isn't "secure" as used in the claims.

III. INTERTRUST'S EFFORTS TO DEFEND "SECURE" REVEAL THE INDEFINITE MEASURE OF SECURITY IMPLICIT IN THE PATENT

InterTrust's proposed solutions to the patent's lack of a standard for "secure" – its Markman definition and or a "commercially reasonability" standard – reveal precisely why the term is indefinite. The evidence confirms that "secure" as used in the claims has no fixed, precise meaning and is constrained by no criteria.

A. The Proposed Markman Definition Is Indefinite

Contrary to its concession of the need for criteria, InterTrust asserts that its proposed *Markman* definition of "secure" is sufficiently definite. InterTrust Opp., at 4. InterTrust's opposition brief omits, however, a crucial sentence within its proposed definition: "Security is not absolute, but designed to be sufficient for a particular purpose." Joint Claim Construction Statement, Exh. A, at 1. The definition states no "purpose," leaving the person of skill in the art completely in the dark as to how much security is needed, or for what, as well as how to measure it.

B. The Proposed Standard of "Commercial Reasonableness" Is Indefinite and Unsupported by the Patent

InterTrust's Opposition brief suggests an alternative definition for "secure" – "commercial reasonability." Having admitted the need for criteria, and challenged to show where the patents provide such criteria, InterTrust asserts that "[t]he information included in the InterTrust patents includes guidance regarding how security should be measured, including the statement that security should be based on a commercially reasonable standard." Opp., 3-4. Dr. Reiter elaborates in his declaration, reiterating the need for context and criteria, but stating that "computer security professionals routinely apply a commercial reasonability standard in building

security into real-world products and in determining whether real-world products or processes are 'secure.'" Reiter SJ Decl., at 12, 18.

If the "commercial reasonability" standard were in fact supported by the patent or the evidence, it would still leave the claims indefinite. But the Court need not even consider that question, because InterTrust's expert, Dr. Reiter, admits that the "commercially reasonable" standard referred to in his second Declaration differs from InterTrust's proposed *Markman* definition. When asked if he drafted the above-quoted sentence about computer security professionals "routinely apply[ing] a commercial reasonability standard," Dr. Reiter responded that he had neither drafted nor dictated it, saying only that he "remember[s] discussing issues like this with InterTrust before this was drafted, as far as I know, because I don't actually know when it was drafted." Reiter Depo., 4/17/03, p. 420:1-20 attached to Wesenberg Reply Decl., Exh. B. That led to the following exchange:

> Q: You recall discussing the opinion that computer security professionals routinely apply a commercial reasonability standard with InterTrust before you arrived at InterTrust and were given the draft of this declaration that's been marked as Exhibit 69?
>
> A. Certainly I remember discussing security is meant to be sufficient for a given purpose or a given set of threats and that requirements for commercial systems would be different than for other types of systems. I don't know if I used exactly the words commercial reasonability standard, though.
>
> Q. Do you understand "commercial reasonability standard" to be synonymous with "designed to be sufficient for a particular purpose"?
>
> A. I don't think I would say they're synonymous.
>
> Q. How do they differ?
>
> A. Commercial reasonability indicates a particular type of purpose or, you know, a particular – I should say maybe set of threats to which protection mechanisms should be robust or against which they should be robust.

Reiter Depo., 4/17/03, pp. 420:21-421:22, Wesenberg Reply Decl., Exh. B. "Commercial reasonability" thus not only means something different from InterTrust's proposed Markman definition, it also (unlike InterTrust's proposed Markman definition) gives at least a general indication what kinds of threats the system is to be secured against.

In fact, the commercial reasonability standard appears nowhere in the patent. Tellingly, Dr. Reiter's declaration does not assert that the patent teaches "commercial reasonability" – only InterTrust's brief makes that claim, citing two excerpts from the specification as support. InterTrust Opp., at 4 n.4. But the cited specification language says nothing about how to evaluate or define "reasonability." Rather, it refers to "sufficient security (sufficiently trusted) for the intended commercial purposes" and states that the level of security **depends on "the commercial requirements of particular markets or market niches, and may vary widely.**" '193, Col. 45:39-45, 49:59-62 (emphasis added). These statements effectively admit that "secure" is indefinite as used in the claims.

C. InterTrust Has Effectively Admitted that Secure Is Indefinite

The patent language that InterTrust cites as support for the "commercial reasonability" standard acknowledges that in these patents the only criteria of "secure" "depends on the commercial requirements of particular markets or market niches, and may vary widely." '193 patent, Col. 49:61-62, quoted in Joint Claim Construction Statement, Exh. C, item 19(B), 19(J), cited in InterTrust Opp., at 4 n.4. This admits indefiniteness, because no measure or method is identified which would let people of skill in the art precisely and reliably reach the same conclusion whether something is "secure" in those admittedly widely varying markets – especially where each of those markets consists of many different companies and people, and many possible different standards and "requirements."

InterTrust's brazenness in taking this position is apparently a function of its confidence that it can overwhelm Microsoft and the Court by citing to the numbing abundance of technical description in its gargantuan patents. The mere presence of voluminous description of possible technologies does not provide the needed measure.

IV. INTERTRUST COINED TERMS "PROTECTED PROCESSING ENVIRONMENT" AND "HOST PROCESSING ENVIRONMENT" AS USED IN ITS PATENTS LACK THE NECESSARY DEFINITENESS TO ONE OF ORDINARY SKILL IN THE ART

Like its arguments regarding "security," InterTrust's arguments regarding Protected Processing Environment ("PPE") and Host Processing Environment ("HPE") miss the

mark. In its Opposition, InterTrust simply ignores its burden of defining coined terms with "precision." *J.T. Eaton & Co. v. Atlantic Paste & Glue Co.*, 106 F. 3d 1563, 1570 (Fed. Cir. 1997). Instead it argues that HPE and PPE receive "extensive discussion in the specification."

Whatever the extent of the discussion, InterTrust points to no instance where these terms are clearly and ***precisely*** defined. Microsoft's primary contention is that when used, the coined phrases HPE or PPE, are used inconsistently, sometimes contradictorily and nearly always shrouded in qualifying and conditional language. The passages from the '193 specification attached to Dr. Reiter's declaration illustrate these defects. First, the nature of, and relationship between, "SPE", "PPE" and "HPE", is indeterminate. In a passage from the '193 specifications and cited by InterTrust's expert, the following relationship is described:

> ROS 602 in this example also includes one or more Host Event Processing Environment ("HPEs") 655 and/or one or more Secure Event Processing Environments ("SPEs") 503 (these environments may be generically referred to as "Protected Processing Environments" 650). (Col. 79, 30-35)

It can be surmised from this that reference to a PPE could mean either SPE or HPE. The specification, however, identifies that "HPEs" may be provided in two types, "Secure" and "Not Secure," and InterTrust leaves one to guess which is which in any given instance. Indeed, InterTrust admits that its proposed definition of HPE does not acknowledge this schism, yet InterTrust offers only a circularity as a remedy: that non-secure HPEs be defined to be HPEs that are not secure.

Any attempt to distinguish these terms by their structural or functional characteristics is futile. When text is actually committed to discussing a "PPE", "SPE" or "HPE" the qualities and/or attribute assigned each are merely optional. In the text following the introduction of the terms PPE and HPE (Col. 79, 31-35) the specification identifies no fewer than four attributes that "may" be aspects of an SPE or HPE. "HPEs and SPEs are self-contained computing and processing environments that ***may include*** their own operating system kernel, ... ***may process*** information in a secure way, ... they ***may*** each perform ... they ***may*** each offer ...". Reiter Decl., Ex. G., p. 2 (Col. 79, 36-46). (Emphasis added.) As demonstrated in this example, representations about functional and design characteristics of HPE's and PPE's are frequently

qualified with the term "may be" or "can be." The first two full paragraphs of Reiter Ex. G at p. 3 when referring to HPEs or SPEs use "may," "may be," "can be" or "could" fifteen times. Every sentence but one does so. The constant use of such qualifying language leaves one irredeemably confused as to the nature and characteristics of the PPEs and HPEs. Again, there is plenty of verbiage directed generally at these terms but they remain undefined, and certainly cannot be understood with anything approximating "precision."

InterTrust's argument that Professor Mitchell "has no difficulty understanding what the term [PPE] means" is both wrong and of no consequence. Microsoft has never disputed that one of ordinary skill in the art would be able to surmise what these coined terms ***might*** suggest when dissected into their component parts. The section of the Mitchell declaration cited by InterTrust is under the caption "what the claim appears to promise." This standard neither purports to, and does not, comport with the requirement of 35 U.S.C. § 112(2).

V. ARGUMENT

A. The Lack of Criteria or Parameters for "Secure" Render It Indefinite

InterTrust's concession that persons of skill in the art require criteria to understand "secure" with any precision, and that there are many different possible sets of criteria, greatly simplifies the analysis in this case. In *Amgen v. Hoechst Marion Roussel, Inc.*, the Federal Circuit held that claim language that could be measured by multiple recognized standards failed for indefiniteness where the written disclosure named several standards but failed to specify which one was to be used. 314 F.3d 1313, 1341-42 (Fed. Cir. 2003). Different methods of purifying human urinary erythropoietin ("uEPO") would produce samples with different glycosylation, which meant that the claim limitation "having glycosylation which differs from that of human uEPO" was a "'moving target.'" *Id.* at 1340, 1341 (quoting lower court). Finding that the specification of the patent "does not direct those of ordinary skill in the art to a standard by which the appropriate comparison can be made," the Court held that "such ambiguity in claim scope is at the heart of the definiteness requirement of 35 U.S.C. § 112 ¶ 2," and affirmed the lower court's finding of indefiniteness. *Id.*, at 1341, 1342. Similarly, the failure of the InterTrust patents to choose from among the many different standards by which "secure" could be

measured, or to specify clear criteria of its own, renders the claims containing the term "secure" and its variants indefinite.

B. Indexing a Claim Term to Market Conditions Creates Impermissible Indefiniteness

Instead of providing a standard, InterTrust has adopted the position that "secure" in this patent "depends on the commercial requirements of different markets or market niches, and may vary widely." That 'criterion' is an unpredictable, moving target, much like the claim term in *Ex parte Brummer*, 12 U.S.P.Q.2d 1653 (B.P.A.I. May 11, 1989). The term at issue in that case depended not on any objectively ascertainable feature, but on the label the manufacturer chose to place on the bicycle reflecting its subjective conception of the customer for whom the product was intended. *Id.*, at 1655. InterTrust's argument that this case is more like *Orthokinetics v. Safety Travel Chairs, Inc.*, 806 F.2d 1565 (Fed. Cir. 1986) is fallacious. In *Orthokinetics*, the term that depended on a factor outside the patent was a length parameter – a one-dimensional variable, so to speak. More importantly, it was not subjective. One of ordinary skill in the art building the claimed travel chair "would easily have been able to determine the appropriate dimensions" by measuring the particular automobile. *Id.* at 1576. The Court therefore found it unnecessary to require the claims to list "all possible lengths corresponding to the spaces in hundreds of different automobiles." *Id.* In *Brummer*, no amount of "listing" in the patent could possibly do the trick, because the terms on which the claim scope depended were subjective – the manufacturer's view of whom the bicycle was intended for, and the characteristics of the rider. Similarly, in this case, a person of skill in the art cannot possibly know what a particular customer, market or market niche will deem sufficiently "secure" until after it has sold the product.

Indeed, the fact that one cannot determine the scope of a claim until a product is first manufactured and sold demonstrates that the terms employing "secure" are also indefinite under the principle of *STX, Inc. v. Brine, Inc.*, 37 F. Supp. 2d 740 (D. Md. 1999), *aff'd* on other grounds, 211 F.3d 588 (Fed. Cir. 2000). In that case, subjective claim language describing a lacrosse stick ("improved handling and playing characteristics") would require one to play with

the stick in order to determine whether it possessed the limitation and therefore infringed. "The notion that one reasonably skilled in the art would have to infringe the patent claim in order to discern *the boundaries of the claim* is repugnant to long-standing principles of patent jurisprudence." *Id.*, at 755. Here too, one would have to manufacture and sell the product to determine whether it would enjoy market success and would thus have "sufficient security for the intended commercial purposes."

C. "Secure" Must Be Definite Because It Is Essential to VDE

InterTrust assails Microsoft for taking the position that the central importance of "secure" to VDE renders it crucial that the term be sufficiently definite. InterTrust Opp., at 20-21. Contrary to InterTrust's argument, Microsoft did not assert a lower standard of proof of indefiniteness; it sought to foreclose any such argument that InterTrust might make. InterTrust's own reading of *Exxon* confirms that noncritical limitations can sometimes be expressed in functional terms, while critical limitations cannot. Moreover, InterTrust's denial that its expert testified that security is "essential to VDE" is false. InterTrust Opp., at 21-22. Asked about "security," Dr. Reiter answered as follows: "I believe it's an essential aspect of VDE as described in the specification, or in the sense that certainly the authors invest a lot of time on questions of security, and so I think that's probably what they had in mind." Wesenberg Reply Decl., Exh. D (Reiter Depo., 2/28/03, at 23:16-20).[3] "Security" is a critical limitation, and must be sufficiently definite.

D. The Use of "Secure" in Other Patents (and Other Contexts) Is Completely Irrelevant to Whether the Claims at Issue Are Definite

It is a well-known aspect of indefiniteness case law that the same terms are held indefinite in some cases, and definite in others. Thus, the question of whether secure may have been used with sufficient definiteness in other patents, articles, etc., is irrelevant to whether it is sufficiently definite here. In holding that a claim using the term "about" was indefinite, the Federal Circuit warned: "In arriving at this conclusion, we caution that our holding that the term

[3] Microsoft's citation of this statement was off by five lines in the opening brief, the citation starting at line 21 instead of line 16 on the same page.

'about' renders indefinite claims 4 and 6 should not be understood as ruling out any and all uses of this term in patent claims. It may be acceptable in appropriate fact situations, even though it is not here." *Amgen, Inc. v. Chugai Pharmaceutical Co., Ltd.*, 927 F.2d 1200, 1218 (Fed. Cir. 1991). Microsoft has never argued that "secure" cannot be used with sufficient definiteness, only that InterTrust's patents fail to do so. InterTrust's arguments about Microsoft's use of "secure" in its patents are irrelevant, as well as mistaken. (For example, the Slivka '671 patent asserted in this case stands in marked contrast to InterTrust's use of "secure" in the claims at issue on this motion, not least because the Slivka '671 patent sets forth a clear standard by which secure or not secure can be evaluated).

1. The Non-Patent Documents that Employ the Term Are Not Required to Satisfy 35 U.S.C. § 112

Equally irrelevant is InterTrust's argument that "secure" is used in myriad publications and other contexts without the specification of every parameter. Microsoft agrees that "secure" is used in the art in many different ways, some quite vague. That is precisely why it is necessary to specify what is meant when using the term in a patent claim. Patent claims must satisfy 35 U.S.C. § 112(2); the publications InterTrust cites need not. (It is worth noting, however, that the only Microsoft publication provided to the Court by InterTrust uses the Common Criteria to evaluate security – in telling contrast to InterTrust's pervasive failure to identify a definite standard or measure by which "secure" can be evaluated by one of skill in the art. *See* Reiter SJ Decl., Exh. J).

VI. INTERTRUST'S EFFORT TO INCORPORATE BY REFERENCE WAS INEFFECTIVE

Patent Office practice surrounding incorporation by reference attempts to balance 1) the need to provide the public a complete written description of the patent (*see, e.g.*, 35 U.S.C. § 112) with 2) "economy, amplification, or clarity of exposition" achieved by allowing lengthy references to be incorporated by reference into an application under certain circumstances. *Ex parte Schwarze*, 151 USPQ 426 (B.P.A.I. 1966); *see* MPEP § 608.01(p). To meet this balance, the Patent Office has directed that: "essential" material may only be incorporated by reference to

an issued U.S. Patent or a published U.S. Patent Application. On the other hand, "nonessential material" may be referred to in a variety of ways. *See* MPEP § 608.01(p). Whether material has been incorporated by reference is a question of law. *Advanced Display Sys., Inc. v. Kent State University*, 212 F.3d 1272, 1282 (Fed. Cir. 2000). InterTrust does not deny that the Big Book material is essential material. The '683, '721, and '861 patents all purport to incorporate the "big book" by reference to the unpublished patent application. For example, the '721 states, "This application is related to commonly assigned copending application Ser. No. 08/388,107 of Ginter et al. . . . We incorporate by reference, into this application, the entire disclosure of this prior-filed Ginter et al. patent application." (721: 1:7-16; cf. 683: 1:7-23; 861 1:7-11). At the time that the applications leading to the '683, '721, and '861 patents were allowed, InterTrust could have easily complied with the appropriate requirement yet chose not to. Here, the '107 application is the "referenced application." The '107 application, in fact, NEVER issued as a patent – so the examiner had no duty to substitute. It is the duty of the applicant to comply with the 112 requirements. *United Carbon Co. v. Binney & Smith Co.*, 317 U.S. 228 (1942). Accordingly, InterTrust should have either taken one of the two simple options that was open to it. It chose not to. Its effort to incorporation by reference was ineffective.

VII. CONCLUSION

For the reasons set forth above, in Microsoft's opening brief and supporting documents and any argument that may be provided at the hearing, Microsoft respectfully ask this Court to grant its motion and find the mini-*Markman* claims to be invalid.

Dated: April 21, 2003

WILLIAM L. ANTHONY
ERIC L. WESENBERG
KENNETH J. HALPERN
ORRICK, HERRINGTON & SUTCLIFFE LLP

Eric L. Wesenberg
Attorneys for Defendant and Counterclaimant
MICROSOFT CORPORATION